SUNRED SECURITY

INCIDENT RESPONDER COURSE MODULE

Delivery: In-person in Brisbane area or remote via Zoom

Course cost: $450 per person

Please contact us if you are able to supply the venue

Outcomes

Finding the confidence for incident response is typically forged in fire, however this isn't a healthy method for growth and often contributes to burnout.

This course gives security analysts the knowledge required to handle the incident response process. We focus on working through scenarios and hands on exercises to gain familiarity in a safe and fun environment.

Throughout the day we develop a incident response plan and finally work through executing the plan in exercises.

The Incident Responder Course Module covers:

We begin the day with an introduction to incident response and talk through the existing frameworks. From here we introduce our sample company and walk through some real world scenarios and how they map to the frameworks.

Working through some examples we investigate how incidents are first detected like through behavioral alerts, security event alerts, endpoint detection and user reports. After this we develop a shared classification of incidents and correlate prioritisation.

We work through each scenario and discuss the containment strategies. We use free and open source tools for lab environments to simulate compromise and eradication. If you would like to integrate the training with a commercial tool that your team uses then please contact us.

From here we focus on the recovery plans, ensuring the business can get back on track with minimal impact and making sure that nothing was missed. We follow up with mock post incident reviews and write up action plans.

Next we focus on incident communication and documentation. We will critique some documentation practices and write some procedures ourselves. Bringing communication methods into the documentation ensures a consistent and clear message to key stakeholders.

Finally we run through some incidents that have happened in the wild. Mapping either to your company or our sample company we run through the full incident response process as a team.

SUNRED SECURITY

INCIDENT MANAGEMENT COURSE MODULE

Delivery: In-person in Brisbane area or remote via Zoom

Course cost: $450 per person

Please contact us if you are able to supply the venue

Outcomes

A large incident at an organisation requires more than a single analyst in incident response. Incident managers learn to pull together multiple teams, set timelines, communicate effectively and resolve incidents with grace.

This course gives an alternative to learning incident management in a safe environment rather than the industry standard of being thrown in the deep end.

The Incident Management Course Module covers:

To start off the day we give a brief overview on incident response frameworks and how incident management fits into the picture. We will establish some real world scenarios where a complex incident requires the involvement of multiple parties and how a effective incident manager ties everyone together.

We run through scenarios where attendees will have to practice incident leadership and communication. We will tie this in with stakeholder management in the exercises.

Begging with each scenario we map incidents to severities in response plans that we create throughout the course. From here we practice resource allocation and prioritisation using a risk based approach.

Afterwards we run through cross team collaboration and delegation practices. Each attendee will get a chance to practice delegation with actionable results and check in times.

For each scenario we formulate methods for recovery plans and incident resolution. We have a strong focus on post-incident reviews and analysis for each scenario, building the lessons learned into our incident response plan.

After working through the practice scenarios on incident management we run through some real world case studies and use it to judge the effectiveness of the plans we develop in the training.

SUNRED SECURITY

TABLETOP EXERCISES COURSE MODULE

Delivery: In-person in Brisbane area or remote via Zoom

Course cost: $450 per person

Please contact us if you are able to supply the venue

Outcomes

Tabletop exercises are a great tool to practice the incident response process but it exists within a wider Test, Training and Exercise (TT&E) program.

This course gives attendees the skills to run a TT&E program at their company and the experience to run tabletop exercises to remember.

The Incident Management Course Module covers:

The days with an overview of TT&E programs and the difference between tabletop and functional exercises. We establish a sample company to run through for scenarios.

Running off our sample company we run with an established threat model to map out capabilities. We move into practical steps by crafting realistic and relevant security scenarios to run as tabletop exercises.

Stepping through a sample tabletop exercise we work backwards to then work out the steps to develop the tabletop exercise. We run tabletop exercise scenarios and work on developing the skills to facilitate the exercises.

Through the end of the tabletop exercises we map out action plans including necessary training as followups. Matching through to action plans the introduction of functional exercises are introduced and discussed.

Finally we assess the outcomes of the exercises and formulate test plans to ensure the effectiveness of the plans. We talk through documentation and policy plans for a TT&E program.

This course is designed to have open room for practicing company specific tabletop exercises at the end of the day.